The UK
Access
Management
Federation
FOR EDUCATION AND RESEARCH

Creating and installing SSL certificates for a Shibboleth on Windows deployment

John Yeaman
Edinburgh's Telford College

These guides have been prepared by organisations who participated in the JANET Shibboleth on Windows project. These guides are provided for general information purposes and are not intended to be definitive or exhaustive guides to the configuration, installation and implementation of Shibboleth On Windows.

Background

Shibboleth secures communications between the user and the IDP using SSL. To secure this port you need to use and configure an SSL certificate. You can use the self signed certificate created when you install Shibboleth on Windows: however, your users will see certificate errors in their browser if this is the case. It is better therefore to use a certificate signed by a Certification Authority (CA). For the CA to authenticate the certificate there must be a chain of certificates from the server's certificate to the certificate belonging to the certificate authority.

In the Java environment these certificates are stored in a keystore. Java provides a tool to administer a keystore called *keytool* which is usually located In the java /bin/ directory.

The instructions below described how to create a java keystore and install a CA-signed certificate.

Creating and installing an SSL certificate in a Java keystore

There are four steps to creating a certificate chain in the key store.

1) Create the keystore and a public & private key
2) Generate a signing request and get it signed
3) Import root and intermediate certs as required
4) Import trusted signed cert from CA

1) Generate Keystore & Public/Private keys

This will create a keystore file called coll.jks and a public and private keypair for the server server.ed-coll.ac.uk with the alias shib.

```
keytool -genkey -alias shib -keystore coll.jks
```

```
Enter keystore password: ******
What is your first and last name?
[Unknown]: server.coll.ac.uk
What is the name of your organizational unit?
[Unknown]: ICT
What is the name of your organization?
[Unknown]: Edinburgh's Telford College
What is the name of your City or Locality?
[Unknown]: Edinburgh
What is the name of your State or Province?
[Unknown]: Midlothian
What is the two-letter country code for this unit?
[Unknown]: GB
Is CN=server.ed-coll.ac.uk, OU=ICT, O=Edinburgh's Telford College, L=Edinburgh,
ST=Midlothian, C=GB
correct? [no]: y
```

2) Generate the signing request file

This will create a certificate signing request called *shib-csr.txt* using the public and private keys shib in coll.jks. The certificate signing request should be forwarded to the Certificate Authority (CA) which will issue your signed certificate.

```
keytool -certreq -file shib-csr.txt -alias shib -keystore
coll.jks
```

Enter keystore password: ******

3) Add root and intermediate certificate to keystore

The root certificate and any intermediate certificate should be obtained from the CA issuing the signed certificate. These are usually available from the CA's website. Ensure you check the fingerprints of any certificate obtained with the CA. Once obtained they should be imported into the keystore.

Import Root Certificate

```
keytool -import -trustcacerts -alias root -file sureserversv.cer -
keystore coll.jks
```

Enter keystore password: ******
Certificate was added to keystore

Import Intermediate Cetificate (May not be required dependant on CA)

```
keytool -import -trustcacerts -alias sureserveredu.cer -file
sureserveredu.cer –keystore coll.jks
```

Enter keystore password: ******
Certificate was added to keystore

4) Import trusted signed cert from CA.

Import the signed certificate which you receive from your CA to keystore.

```
keytool -import -trustcacerts -alias shib -file shib.ed-
coll.ac.uk.pem -keystore coll.jks
```

Enter keystore password: ******
Certificate reply was installed in keystore

References

http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html

Disclaimer

This guide is provided by JANET(UK) for general information purposes only and the JNT Association cannot accept any responsibility and shall not be liable for any loss or damage which may result from reliance on the information provided in it.